Defense-in-Depth

ISSUE 2: How to specify defense-in-depth for non-light-water reactors (i.e., should a description be developed?).

BACKGROUND:

The philosophy of defense-in-depth (DID) has been a fundamental part of NRC's regulatory programs since NRC's inception. It is mentioned in numerous places, including the Safety Goal Policy Statement, the probabilistic risk assessment (PRA) Policy Statement and the Commission's 1999 White Paper on Risk-Informed, Performance-Based Regulation. However, the specific elements that constitute DID are not described. The current regulations are also based upon a philosophy of DID; however, the only places the term DID is used in the regulations are in 10 CFR Part 50, Appendix R, Fire Protection, and 10 CFR Part 100.1, Reactor Site Criteria.

It should be recognized that compliance with the regulations ensures DID for light-water reactors (LWRs). The goal of DID is best described by the definition in the Commission's 1999 white paper on risk-informed, performance-based regulation which states: "Defense-in-depth is an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally-caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges." In addition, Regulatory Guide 1.174 contains a discussion of DID and those elements of DID that need consideration when proposing risk-informed changes to a plant's current licensing basis, however, the focus of the discussion is on assessing changes to DID, not defining it.

Others have attempted to describe the elements of DID. Examples include the International Atomic Energy Agency (IAEA) and the International Nuclear Safety Advisory Group (INSAG) in their documents:

- IAEA Safety Series US-R-1, "Safety Assessment and Verification for Nuclear Power Plants," 2001.
- IAEA-TECDOC-986, "Implementation of defense in depth for next generation light water reactors," December 1997.
- Safety Series No. 75-INSAG-3, "Basic Safety Principles for Nuclear Power Plants," 1988.
- Safety Series No. 75-INSAG-3, Rev. 1, INSAG-12, "Basic Safety Principles for Nuclear Power Plants," 1999.

These documents describe DID as having a series of levels, with each level building upon the previous one. The levels contain programmatic as well as physical elements. ACRS, in a letter dated May 19, 1999, discussed the role of DID in a risk-informed regulatory system. In that letter they discuss two fundamental approaches to DID, which they call structuralist and rationalist. The structuralist approach is mainly one of deterministic engineering judgement regarding what constitutes the elements of DID and could be developed generically or on a plant-specific basis, and the rationalist approach is mainly one utilizing a PRA whereby the elements of DID are those items necessary to compensate for uncertainties identified by a plant-specific PRA, such that design and performance goals can be met. Finally, the Nuclear Energy Institute (NEI), in its white paper on "A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors," has proposed that DID be considered a process to account for uncertainties and applied on a design-specific basis.

DISCUSSION:

With the LWR orientation of the current regulations, application of the DID philosophy for non-LWRs has, in the past, been done on a case-by-case basis. With the potential for future plant applications, some of which could be non-LWRs or LWR designs very different from current LWR designs, it may be appropriate to consider developing more explicit guidance describing the DID philosophy as it pertains to reactor design and operation. This could help ensure a more uniform application of the DID philosophy in the future (either on a plant-specific basis or generically) and could also be of use in other areas where DID is important, such as the Regulatory Analysis Guidelines (NUREG/BR-0058, Rev. 3). If more explicit guidance is developed, a fundamental question then becomes what are considered the elements of DID? For example, do they include programmatic as well as physical elements? The development of more explicit guidance would also support development of a framework for future plant licensing and the dissemination of such guidance could be through a policy statement or white paper such that it receives broad visibility and application.

At the public workshop held October 22–23, 2002, there was broad support for developing a description of DID as long as the development was done through a process that included opportunity for public review and comment.

OPTIONS:

The options considered by the staff in addressing this issue are:

(a) Assess DID on a case-by-case basis as part of the review of a specific design (i.e., do not develop a description).

This option would, in effect, maintain the status quo with no specific guidance on DID, other than what is necessary to include in the framework for future plant licensing. The need for design or programmatic features to compensate for uncertainties would be decided case-by-case based upon confidence in the design, including its supporting research and development, and worldwide experience. This option would not ensure uniform application of DID among designs nor would it provide guidance on DID for use in other activities, such as the Reactor Oversight Program or the Regulatory Analysis Guidelines.

(b) Develop a policy statement or description (e.g., white paper) of the elements considered as DID as guidance to designers and the staff.

This option would, in effect, implement the Commission's definition of DID contained in the March 11, 1999, White Paper on RIPB Regulation. It would describe those elements (which could be a combination of structuralist and rationalist elements, and include programmatic as well as hardware-related items) necessary to ensure DID and could be useful in the design, review and oversight process. It could also be useful in other areas such as regulatory analysis. The documentation of the DID description could be in the form of a Commission Policy Statement, White Paper or other high-level document. The policy statement or description would be technology neutral and risk-informed and written to describe:

- the objectives of defense-in-depth (philosophy)
- the scope of defense-in-depth (design, operation, etc.)
- the elements of defense-in-depth (high level principles and guidelines)

The advantage of this option is that it would help ensure uniform application of DID by designers and the staff and would establish a set of attributes that the plant would have to have no matter what the design or calculated risk. This could contribute to public confidence. As part of developing a framework for future plant licensing, as discussed in the Advanced Reactor Research Plan,[1] DID considerations will be included. A comprehensive description of DID could form a structure from which to develop the framework for future plant licensing. This framework could then be used to implement the DID description and to guide future plant reviews, either on a case-by-case basis or through a generic action to codify the framework, if it is decided to take such a generic action.

(c) Develop a programmatic process to ensure DID is implemented in reactor designs.

This option would be similar to that proposed by NEI in their May 2002 white paper on "A Risk-Informed, Performance Based Regulatory Framework for Power Reactors." It would not specify any specific DID plant features but rather would set up a process to be followed by designers and the staff whereby a design could be evaluated against a set of criteria and, depending upon uncertainties in the analysis, additional features or actions would be added to reduce the uncertainty. These additional plant features or actions would be considered DID, and the DID process would, in effect, be a way to treat uncertainties. This process could be documented in various ways, similar to Option (b) above. This option would provide flexibility in the application of DID to different designs and could be a process applicable to non reactor activities as well. Its disadvantages are that it could be subject to non-uniform application and it does not specify any specific attributes that must be included as part of DID (e.g., two ways to accomplish reactor shutdown).

[1]A draft of the Advanced Reactor Research Plan was provided to the Commission in July 2002. A final version will be provided in April 2003.

(d) Develop a policy statement or description (e.g., white paper) of DID that could include specific technical elements as well as process elements as guidance to designers and their staff.

This option is a combination of options b and c above and is put forth in recognition of the fact that in developing the policy statement or description of DID, input will be received from stakeholders that could influence the scope and content of the DID description. Accordingly, the elements of DID could be technical and/or process and will be determined as part of developing the DID policy statement or description.

Nevertheless, the policy statement or description would be written to be technology neutral and risk-informed and address:

- the objectives of defense-in-depth (philosophy)
- the scope of defense-in-depth (design, operation, etc.)
- the elements of defense-in-depth (high level principles and guidelines)

RECOMMENDATION:

The staff recommends the Commission take the following actions:

- Approve the development of a policy statement or description (e.g., white paper) on defense-in-depth for nuclear power plants to describe:

  - the objectives of defense-in-depth (philosophy)
  - the scope of defense-in-depth (design, operation, etc.)
  - the elements of defense-in-depth (high level principles and guidelines)

  The policy statement/description would be technology neutral and risk-informed and would be useful in providing consistency in other regulatory programs (e.g., Regulatory Analysis Guidelines).

- Develop the policy statement/description through a process involving stakeholder review, input and participation.

This recommendation is consistent with Option d above. Given the fundamental nature of the defense-in-depth philosophy to reactor safety, it is recommended that the Commission articulate the elements of this philosophy in a fashion that receives wide distribution and visibility. A description of DID would help provide consistency to the application of DID and coherence with other regulatory activities that include consideration of DID (e.g., Regulatory Analysis Guidelines). Clearly, such a description would need to be assessed for its implications for future LWRs. The schedule for developing such a description would likely be 1 year considering the need for stakeholder input, ACRS review, and internal review and comment.